Jiahui **Lu**

(+1) 404-429-2362 | lujiahui1@hotmail.com | alanwap.github.io | AlanWaP | AlanWaP

Education

Georgia Institute of Technology (Georgia Tech) — *Atlanta, Georgia, US*

MS in Computer Science — *Aug 2017 - Dec 2021*

- Institute for Information Security & Privacity, College of Computing
- G.P.A. 3.84/4.0

Shanghai Jiao Tong University (SJTU) — *Shanghai, China*

BSE in Computer Science — *Sept 2013 - July 2017*

- ACM Honored Program, Zhiyuan College
- G.P.A. 3.77/4.3

Work Experience

Inspur USA Inc. — *Mountain View, California, US (Remote in Atlanta, GA, US)*

Software Engineer — *Aug 2022 -*

- Developing command line tool for database server
- Implementing subscription system for cloud service
- Implementing distributed database engine product

JD.com Silicon Valley R&D Center — *Mountain View, California, US (Remote in Atlanta, GA, US)*

Research Scientist & Architect — *Feb 2022 - Aug 2022 (Lab shut down)*

- Developed secure neural network system with multi-party computation (MPC) frameworks (ABY, Falcon, etc.)
- Explored scenarios of fully homomorphic encryption in private computing services, e.g. generating multiplication triples

JD.com Silicon Valley R&D Center — *Mountain View, California, US (Remote in Atlanta, GA, US)*

Research Intern — *May 2021 - Aug 2021*

- Implemented a protocol to generate distributed RSA secret key pair securely between two servers using oblivious transfer

Research Experience

Institute for Information Security & Privacity, Georgia Tech — *Atlanta, Georgia, US*

Graduate Research Assistant — *Aug 2017 - Dec 2021*

- Advisor: Prof. Alexendra Boldyreva & Prof. Vlad Kolesnikov
- Designed secure review protocols supporting instant authorization and user anonymity
- Optimized a zero knowledge proof scheme using MPC-in-the-head to satisfy efficient boolean and arithmetic operations

Security & Privacy group, Cornell Tech — *New York City, New York, US*

Research Intern — *Aug 2016 - Dec 2016*

- Advisor: Prof. Tom Ristenpart
- Explored side-channel attacks in full text search systems
- Analyzed the security of symmetric encryption schemes as cryptographic commitments

Cornell University — *Ithaca, New York, US*

Exchange Student — *Jul. 2012 - Jun. 2013*

- Advisor: Prof. John E. Hopcroft
- Explored the role of units in different convolutional layers of a deep learning network

Lab of Cryptology and Computer Security, SJTU — *Shanghai, China*

Undergrad Research Assistant — *Jun 2015 - Jun 2016*

- Advisor: Prof. Yu Yu
- Explored problems related to Learning Parity with Noise and Fully-Homomorphic Encryption

Publication

Efficient Generic Arithmetic for KKW - Practical Linear MPC-in-the-Head NIZK on Commodity Hardware without Trusted Setup

International Symposium on Cyber Security Cryptology and Machine Learning - CSCML 2021

- Authors: David Heath, Vladimir Kolesnikov, Jiahui Lu
- Conference Talk

Message Franking via Committing Authenticated Encryption

Advances in Cryptology - Crypto 2017

- Authors: Paul Grubbs, Jiahui Lu, and Thomas Ristenpart

Side-Channel Attacks on Shared Search Indexes

IEEE Symposium on Security and Privacy - Oakland 2017

- Authors: Liang Wang, Paul Grubbs, Jiahui Lu, Vincent Bindschaedler, David Cash, Thomas Ristenpart

Anonymous Review Systems for (Un)linkable Settings

In progress

- Authors: Alexandra Boldyreva, Jiahui Lu

Honors & Awards

Qualified to 3rd Round in the 2021 Google Code Jam

Online

Individual

May 2021

4th place in the 2018 ACM-ICPC Southeast USA Regional Contest

Kennesaw, Georiga, US

Team BuShiMeiguoRen, Georgia Tech

Nov 2018

- 1st in Kennesaw State University site

9th place in the 2018 ITA Tech Challenge

Chicago, Illinois, US

Individual

Oct 2018

2nd place in the 2018 Mercer University Spring Programming competition

Macon, Georiga, US

Team Yellow Jackets, Georgia Tech

Feb 2018

- 1st in Division II

Extracurricular Activities

ACM programming team, Georgia Tech

Atlanta, Georgia, US

Coach

Aug 2019 - Dec 2021

- Team meeting lecturer
- College team representative in contests. Participated in
  - 2020 Mercer University Spring Programming competition
  - 2020 Southeast USA Regional Contest
  - 2021 ICPC North America Division Championships
  - 2021 ICPC North America Championships

2020 Mercer University Spring Programming competition

Macon, Georgia, US

Staff & Problem writer

Feb 2020

ISNDES

Online

Website admin

Aug 2018 - Aug 2020

- Front-end developer of a fan-made forum www.isndes.com

ACM programming team, Georgia Tech

Atlanta, Georgia, US

Contestant

Aug 2017 - Aug 2019